REMARKS

Claim 1-20 are pending in the present application.

The Applicant filed the original application on April 5, 2001.

The Examiner mailed the first, non-final Office Action dated September 24, 2004, wherein claims 1-5, 7-20 were rejected under 35 USC 102(e) as being anticipated by Krishna.

The Examiner mailed a second, non-final Office Action dated March 24, 2005, wherein claims 1-20 were rejected under 35 USC 103(a) as being unpatentable over Jones in view of King.

The Examiner mailed a third, non-final Office Action dated September 8, 2005, wherein claims 1-20 were rejected under 35 USC 103(a) as being unpatentable over Boneh in view of Jones.

The Examiner mailed a fourth, final Office Action dated June 2, 2006, wherein claims 1-20 remain rejected under 35 USC 103(a) as being unpatentable over Boneh in view of Jones.

The Examiner mailed an Advisory Action dated September 28, 2006 maintaining the rejection in the final Office Action dated June 2, 2006.

The remarks herein are in response to the fourth Office Action.

Rejection under 35 U.S.C. 103(a)

Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boneh, et al (Pub. No. 2002/0112167) (Boneh) in view of Jones, et al. (U.S. Patent No. 6,088,800) (Jones).

The applicant respectfully amends the present claims 1-20 and traverses the rejection. The applicant respectfully submits that the differences between the subject matter sought to be patented and the references cited by the Examiner are not such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains.

As succinctly stated in the MPEP, to establish a prima facie case of obviousness, three basic criteria must be satisfied:

"First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claimed limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on the applicant's disclosure." Section 706.02(j) (citing *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

"To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." MPEP 706.02(j) (quoting *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)).

<u>Teachings of Boneh:</u>

Boneh teaches, in the Abstract: "A method and apparatus are provided for *protecting sensitive information within server* or other computing environments. Numerous electronic requests addressed to a server system are received over network couplings and evaluated. The evaluation scans for sensitive information including credit card information and private user information. Upon detecting sensitive data, *cryptographic operations are applied to the sensitive data.* When the sensitive data is being *transferred to the server system*, the *cryptographic operations encrypt the sensitive data prior to transfer* among components of the server system. When sensitive data is being *transferred from the server system*, the crypto*graphic operations decrypt the sensitive data prior to transfer* among the network couplings. The cryptographic operations also include hash, and keyed hash operations." (emphasis added)

Boneh teaches that one or more TE Appliances (e.g., 102, 202, 204) perform the encryption and/or decryption.

Boneh teaches that function of the TE Appliances may be dedicated network appliances or distributed among various associated network components (page 2, par. 0027)

Boneh teaches: "When the TE Appliance identifies tags indicating that the associated data is sensitive, it applies an *appropriate cryptographic operation* to the data within these tags, in block 306. For example, incoming sensitive data is *encrypted using known encryption algorithms* such as know public key infrastructure ("PKI") encryption algorithms or the Data Encryption Standard ("DES")." (page 2, par. 29) (emphasis added)

Boneh, at page 5, par. 0061 and 0062, as cited by the Examiner, merely provides a general description of a "processor," including CPUs, DSPs, and ASICs, and a general description of a "computer-readable media," respectively.

Teachings of Jones:

Jones teaches three *known encryption algorithms*, including DES and RC5 (both standard IPSEC algorithms), and IDEA (i.e., a PGP encryption algorithm). (col. 5, lines 49-53)

Jones describes an "encryption chip" (see Fig. 2) having an "encryption/decryption *pipeline*. . . made up of a plurality of processing elements 37 arranged in a linear array, each containing an instruction memory, a register file, an ALU, local and shared data memory, and control circuitry." Jones, col. 6, ll. 7-13 (emphasis added).

Applicant's response to the Examiner's Final Office Action and Advisory Action:

In rejecting claim 1, the Examiner sets forth two different arguments.

Firstly, under the "Rejection" on page 6 of the Final Office Action, the Examiner states that Boneh teaches all of the limitations in claim 1, except a multi-layer protocol, which is taught by Jones (Jones, col. 5, lines 44-53).

Secondly, under the "Response to Arguments" on page 2 of the Final Office Action, the Examiner states that Boneh in view of Jones teaches "means for implementing cryptographic acceleration function of a software application having using the security protocol IPSec" (Jones, col. 5, lines 44-53). Data can be transferred among processors operating one layer of the multi-layer protocol such as IPSec and SSL by utilizing operands of the encryption pipeline processor (Jones, col. 6, lines 18-28). Boneh teaches a high performance processor, such as a digital signal processor, operating on one layer of an SSL protocol. (page 5, par. 0061). Boneh and Jones further teach the means for accessible memory to each of the processors passing operands. (Boneh page 5, par. 0062 and Jones, col. 7, lines 15-34)."

Regardless of which of the two arguments that the Examiner applies, the Examiner has failed to provide a proper rejection under section 103(a) for the following reasons.

Boneh's TE Appliances that perform the encryption and/or decryption lack the "mobile device", as well as "a high performance processor configured to operate one layer of the multi-layer protocol for the benefit of the first processor according to a command from the first processor," as claimed by Applicant. Boneh also lacks the "memory accessible to each of the first processor and the high performance processor for passing commands and data between the first processor and the high performance processor" as claimed by Applicant.

Jones' encryption chip lacks the "mobile device", as well as "a high performance processor configured to operate one layer of the multi-layer protocol for the benefit of the first processor according to a command from the first processor," as claimed by Applicant. Jones also lacks the "memory accessible to each of the first processor and the high performance processor for passing commands and data between the first processor and the high performance processor" as claimed by Applicant.

In rejecting claim 1, it appears that the Examiner cited the "processing element(s)" and/or the "control CPU 52" of Jones as teaching the first and high performance processors of claim 1 – although it is not entirely clear from the cited text – and the memory elements of the "processing elements" of Jones as teaching the memory element of claim 1.

Each processing element ("PE") 37 in Jones:

> consists of an ALU 56 operating on 32-bit words from a register file 58 made up of 8-16 32 bit registers. The register file 58 and ALU 56 *are controlled by a control unit 60 which decodes instructions from a processing element instruction memory 62.* Each processing element instruction memory stores at least one round of an encryption algorithm, where a round is defined as a sequence of instructions in an encryption algorithm.

Jones, col. 7, ll. 17-25, and Fig. 3 (emphasis added). There is *no distinction* from one processing element in Jones to the next. One processing element is *not* a "first processor operating a software application having a multi-layer protocol" while another is "a high performance processor configured to operate one layer of the multi-layer protocol for the benefit of the first processor according to a command from the first processor." All of the processing elements in the pipeline are identical, where each processing element implements a round of an encryption code algorithm. Jones, col. 6, ll. 44-52.

No commands are passed from one processing element to another via a memory, such as in claim 1, "accessible to each of the first processor and the high performance processor." The register file and ALU of each of Jones' processing elements are controlled by a control unit local to each processing element which obtains its instructions from an instruction memory, also *local* to each processing element. See also, Jones, Fig. 3.

The control CPU 52 described by Jones, merely "synchronizes the operations of the encryption pipeline processors." Jones, col. 6, ll. 26-28. "Furthermore, to allow processing of algorithms which utilize very wide operands such as public-key encryption algorithms, a public-key (PK) core processor 46 is connected to the control CPU 52." Jones, col. 6, ll. 29-33. "Other instructions necessary for implementing PK algorithms can be executed within the control CPU 52." Jones, col. 6, ll. 41-43. In other words, the CPU 52 and associated PK core processor certainly are *not* configured to operate one layer of the multi-layer protocol according to a command from a first processor, as claimed by Applicant in claim 1.

The Examiner cites Jones at col. 7, lines 15-34 for teaching a memory for passing commands and data between the first processor and the high performance processor. However, at this citation, Jones describes the contents of each "processing element" in the pipeline, as shown in FIG. 3. Further, Jones' teaching at column 6, lines 3-18 describes the contents of each "processing element" of Jones in the pipeline. The only reference to memory in this portion of Jones is in column 6, lines 10-13 where it states, "the pipeline is made up of a plurality of processing elements 37 arranged in a linear array, each containing an instruction memory, a register file, an ALU, local and shared data memory, and control circuitry." The local and shared data memory of each processing element (elements 64, 66, and 68 of Jones, Fig. 3 respectively) function to serve the local processing element and those immediately adjacent to it in the pipeline. "The [shared] memories 66 and 68 of a processing element are dual port SRAMs and are shared with the PE of the previous and next pipe stage, respectively." Jones, col. 7, ll. 40-42. Therefore, the local and shared data memories of each processing element of Jones do not pass commands and data between a first processor and a high performance processor, as claimed in claim 1.

Boneh describes a DSP and a computer-readable memory at page 5, sections 0061 and 0062, respectively. However, Boneh does not teach or suggest that the DSP is "configured to operate one layer of the multi-layer protocol for the benefit of another processor according to a command from the other processor," as claimed in claim 1. Further, Boneh does not teach or suggest that the computer-readable memory is "accessible to each of the first processor and the high performance processor for passing commands and data between the first processor and the high performance processor," as claimed in claim 1.

The combination of Boneh in view of Jones does not meet the limitations of claim 1. All of the processing elements in the pipeline are identical, where each processing element implements a round of an encryption code algorithm. Jones, col. 6, ll. 44-52. The control CPU 52 described by Jones, merely "synchronizes the operations of the encryption pipeline processors." Jones, col. 6, ll. 26-28. The [shared] memories 66 and 68 of a processing element are dual port SRAMs and are shared with the PE of the previous and next pipe stage, respectively." Jones, col. 7, ll. 40-42. Boneh describes a DSP and a computer-readable memory (page 5, sections 0061 and 0062), but they are not used according to the claimed limitations. Therefore, the combination of Boneh in view of Jones lacks the claimed limitations: "mobile device," "a high performance processor configured to operate one layer of the multi-layer protocol for the benefit of the first processor according to a command from the first processor," and "memory accessible to each of the first processor and the high performance processor for passing commands and data between the first processor and the high performance processor" as claimed

The obviousness rejection of Boneh in view of Jones for claim 1 by the Examiner is unsupported by the cited art and should be withdrawn. As independent claim 1 is distinguished over Boneh in view of Jones, dependent claims 2-6 are similarly distinguished.

Regarding independent claim 7, the Applicant submits the following arguments in addition to the arguments with reference to claim 1. The Examiner cited Jones, column 6, lines 3-17 as teaching the "high performance processor coupled to the memory and operating a second portion of the predetermined one of the security protocols for the benefit of the processor via the shared memory" element of claim 7. However, no mention of a high performance processor is made anywhere in Jones. As stated above, all of the processing elements of Jones are identical, none of which are high performance. Each of the processing elements in the pipeline implements *a round* of an encryption code algorithm. Jones, col. 6, ll. 44-52. Each processing element ("PE") 37 in Jones "consists of an ALU 56 operating on 32-bit words from a register file 58 made up of 8-16 32 bit registers." Jones, col. 7, ll. 18-20. Boneh describes a DSP (page 5, sections 0061), but the DSP not used according to the claimed limitations. None of the basic criteria for an obviousness rejection have been met by reference to Jones. The obviousness rejection of claim 7 is unsupported by the cited art and should be withdrawn. As independent claim 7 is distinguished over Jones, dependent claims 8-11 are similarly distinguished.

Regarding independent claim 12, the Applicant submits the following arguments in addition to the arguments with reference to claim 1. The Examiner cited Jones, column 17, lines 7-12 as teaching the "one or more application program interfaces. . ." element of claim 12. Jones does not have such interfaces because Jones describes only a pipeline of processing elements, each of which implements *a round* of an encryption code algorithm. Jones, col. 6, ll. 44-52. Lines 7-12 of column 17 in Jones describe the expansion operation of a DES (data encryption standard) encryption routine, which has nothing to do with "one or more application program interfaces operated by the first processor core for interfacing between the security services protocol and the second processor core."

None of the basic criteria set forth above for an obviousness rejection have been met by reference to Jones. The obviousness rejection of claim 12 is unsupported by the cited art and should be withdrawn. As independent claim 12 is distinguished over Jones, dependent claims 13-14 are similarly distinguished.

Regarding independent claim 15, the Applicant submits the following arguments in addition to the arguments with reference to claim 1. The Examiner cited Jones, column 6, lines 44-67, and column 7, lines 1-14 as teaching the partitioning, distributing, and performing steps of the claimed method. Again, as discussed in detail above, Jones does not teach, suggest, or describe partitioning a function of a multi-layer protocol over to a high performance processor. The cited text of Jones describes the processor element pipeline that "implements the code for each round of a secret key algorithm." Jones, col. 6, ll. 44-45. Jones, column 7, lines 25-38, cited by the Examiner, as teaching the returning step of the claimed method, actually describes the local, shared, and global memories of the Jones encryption chip. Again, Jones makes no mention of "returning a result of the distributed function from the high performance processor to the first processor via the shared memory."

The obviousness rejection of claim 15 is unsupported by the cited art and should be withdrawn. As independent claim 15 is distinguished over Boneh in view of Jones, dependent claims 16-20 are similarly distinguished.

In addition to traversing the Examiner's rejection, the Applicant amends each of the independent claims 1, 7, 12, and 15 to indicate that the invention is implemented in a mobile device, and that the high performance processor operates for the benefit of another processor. The dependent claims are also amended to provide proper antecedent basis. The Applicants submits that these amendments further distinguish the present claims from Boneh in view of Jones.

Boneh describes system distributed in a network, as shown in FIG. 4, for example. Although Boneh mentions that aspects of the Boneh's invention may be implemented in a "cellular or mobile phone," Boneh does not teach or suggest how the network configuration of FIG. 4, including the TE appliances 402 and 404, could be modified to implement Boneh's invention in a cellular or mobile phone.

Neither Boneh or Jones teach or suggest that a high performance processor operates for the benefit of another processor, as claimed.

According to the present specification, for example, the system architecture of the circuit 10 takes advantage of the processing power of the DSP 14 and the ability of the DSP 14 to perform certain functions quickly. In wireless communications applications, in particular, the processing power of the DSP 14 is utilized to off-load the CPU 12 and accelerate the complex encryption and authentication algorithms within security protocols. Accordingly, the system architecture of the circuit 10 partitions the cryptographic layers of the security protocols and distributes them to the on-board DSP 14, which returns the result to the CPU 12 in a timely manner without increased equipment costs to the customer. (page 17, lines 14-24)

In view of the foregoing, Applicant submits that all pending claims are in condition for allowance. Applicant respectfully requests the reconsideration and reexamination of this application and the timely allowance of the pending claims. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

If there are any other fees due in connection with the filing of the response, please charge the fees to our Deposit Account No. 17-0026. If a fee is required for an extension of time under 37 CFR 1.136 not accounted for above, such an extension is requested and the fee should also be charged to our Deposit Account.

Applicants therefore respectfully request that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

Dated: November 2, 2006

By: \Donald C. Kordich\
Donald C. Kordich
Attorney for Applicant
Registration No. 38,213

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121-2779
Telephone: (858) 658-5928
Facsimile: (858) 658-2502